A publication of the DCIS Northeast Field Office

TECHNOBABBLE

The DCIS Cyber Crime Newsletter

TECHNOBABBLE
Volume 3, Issue 2

March, 2002

This issues suggested computer crime bookmarks:

Secret Service Electronic Crimes Task Force Page:

http://www.ecTaskForce.org

Electronic Privacy Information Center Computer Security Page:

http://www.epic.org/security/

The Computer Security Institute :

http://www.gocsi.com

Inside this issue:

Secret Service forms Electronic Crimes Task Forces

The United States Secret Service has launched an initiative whereby the agency will form eight new Electronic Crimes Task Force branches throughout the country, including a Boston, MA based branch. The Service is actively soliciting private sector and corporate participation.

"I've been doing things with the U.S. Secret Service for many years now, and this is the most ambitious outreach program that I've seen so far," stated Jack Wiles, President and co-founder of TheTrainingCo, and a corporate participant in the task force. "Over the years, a number of people have asked me about the perceived danger of having everything that we say to them turned into the proverbial 'federal case.' I can honestly say that I have never seen or personally heard of that happening. Not one single person that I know of has ever had their computer(s) seized or even been inconvenienced as a result of trying to do some things to help or even asking for help. This is a group that does a lot more to help prevent, or when necessary convict and hopefully bring to prosecution, these new crimes that are impacting just about everything that we do."

NEW YORK ROOTS

The new task forces will be loosely based upon a concept which Special Agent Bob Weaver of the USSS field office in New York developed in 1995. Since formation of the New York Electronic Crimes Task Force (NYECTF), it has grown to include 100 private companies, 12 universities, and over 50 local, state and federal law enforcement agencies including the U.S. Customs Service, the Internal Revenue Service (IRS), the Bureau of Alcohol, Tobacco & Firearms (ATF), and the Defense Criminal Investigative Service (DCIS). The task force is generally regarded as one of the most successful private sector-law enforcement corroborative efforts ever developed. According to the Secret Service, at the November 2001 meeting of the NYECTF, over 450 members were in attendance.

NEW LOCATIONS

Eight cities, including New York, will be home to the new Electronic Crime Task Forces. ECTF's will be located in:

Boston, Massachusetts
Charlotte, North Carolina
Chicago, Illinois
Las Vegas, Nevada
Miami, Florida
New York, New York
San Francisco, California
Washington, DC

TOP DOWN SUPPORT

Protecting U.S. consumers from electronic and computer based crime has been deemed a priority at the highest levels of the Secret Service. "It may surprise readers to learn that the United States Secret Service is actively engaged in the fight against Internet crime and computer-based fraud," stated Secret Service Director Brian L. Stafford in a web based article. "If asked what they know of the Secret Service, most Americans would likely point to the special agent with the sunglasses and earpiece standing behind the president. They would not imagine that many of those same agents who protect our highest elected leaders are also responsible for protecting consumers against criminal activity on the Internet."

According to Stafford, the success of the ECTF's is highly dependent upon private sector involvement. "If we are serious about computer crime prevention, law enforcement must enlist the technical resources and expertise of the private sector and academia. By complementing those assets with our own expertise and investigative abilities, this unprecedented alliance in New York has achieved remarkable success and has provided us with the blueprint we need to combat cyber crime."

For more information, check out www.ecTaskForce.org.

To contact the USSS Boston based ECTF with questions, call Supervisory Special Agent Jim Perro at (617)565-5640, or drop an e-mail to bostecc@usss.treas.gov.

Former DEA Agent Charged with Computer Crime Flees

A former Drug Enforcement Administration (DEA) special agent charged with selling data obtained from sensitive law enforcement computers has skipped bail.

Emilio Calatayud had been free on a $100,000 property bond since January, 2001 when he was charged with wire fraud, bribery, and violation of the Computer Fraud and Abuse Act for allegedly selling criminal history and other law enforcement information to private investigations firm Triple Check Investigative Services in Los Angeles.

Through his position as a DEA special agent, Calatayud had access to the FBI's National Crime Information Center (NCIC), which maintains nationwide records on arrest histories, convictions and warrants; the California Law Enforcement Telecommunications System (CLETS), a state network that gives agents access to California motor vehicle records and criminal histories, and a DEA system known as the Narcotics and Dangerous Drug Information System (NADDIS).

The case was investigated by the FBI, the Justice Department, the IRS, and the DEA's Office of Professional Responsibility.

(CNN)

Calatayud's trial was scheduled to begin Tuesday, February 5th, but the former agent failed to appear.

According to prosecutors, Calatayud sold information from 1993 through 1999. He allegedly received from $1,080 to $8,500 annually for the information supplied to the PI firm each year.

Computerized National Alert System to be Unveiled

Reprinted from Government Computer Week
February 25, 2002
By Dibya Sarkar

Tom Ridge, head of the Office of Homeland Security, said the federal government would unveil a national alert system in a "couple of weeks" to better share intelligence information about possible acts of terrorism with states and territories.

The former Pennsylvania governor spoke at the National Governors Association's (www.nga.org) winter meeting in Washington, D.C., Feb. 24. Ridge called the national alert system an "imperfect system" that will need improvement. He said the federal government will not mandate use of this system, and he asked for input from state and territorial governments. He asked the governors to take a look at it, compare it with their systems and make recommendations.

"That national system will have to be based on consent," he said.

The federal government has been working on a national system to better rank potential terrorist threats. State and local officials have criticized the warnings that have been issued since Sept. 11 because they contained no details of when and where such acts may occur. California Gov. Gray Davis proposed a national four-stage alert system last year. But at the time, Ridge reportedly asked Davis to delay his proposal so that the federal government could work on a national model.

According to the NGA Web site, such an alert system would categorize credible threats as Stage 1, confirmed threats as Stage 2, confirmed threats on specific locations as Stage 3, and confirmed threats within a specific time frame as Stage 4. The International Association of Chiefs of Police has proposed a similar model.

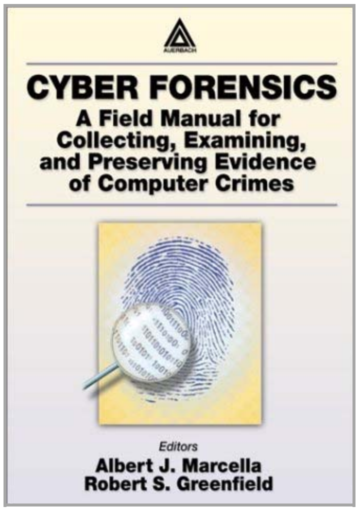
"The challenge of processing and analyzing the bits and pieces of information that get before the intelligence community and FBI is more complex than these professionals get credit for," Ridge said. "They're doing a far better job today than on Sept. 11."

Ridge said assessing and corroborating information and then sharing it is not an easy task. It's a cultural challenge as well as a technological one, and the infrastructure is not yet set up to handle subjective analysis and dissemination of information. "It's as much art as it is science," he said.

"The challenge of processing and analyzing the bits and pieces of information that get before the intelligence community and FBI is more complex than these professionals get credit for," Ridge said. "They're doing a far better job today than on Sept. 11."

This Issues Suggested Reading

Cyber Forensics—A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes


CYBER FORENSICS
A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes
Editors
Albert J. Marcella
Robert S. Greenfield

Looking for a text that goes beyond addressing the basics of computer forensic collection techniques? *Cyber Forensics* may be just the book for you.

An Amazon.com Editorial Review states :

> "*Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes* provides a comprehensive, highly usable, and clearly organized resource to the issues, tools, and control techniques needed to successfully investigate illegal activities perpetuated through the use of information technology. Traditional forensics professionals use fingerprints, DNA typing, and ballistics analysis to make their case. Infosec professionals have to develop new tools for collecting, examining, and evaluating data in an effort to establish intent, culpability, motive, means, methods and loss resulting from e-crimes. The field bible for infosecurity professionals, this book introduces you to the broad field of cyber forensics and presents the various tools and techniques designed to maintain control over your organization. You will understand how to:

o Identify inappropriate uses of corporate IT.

o Examine computing environments to identify and gather electronic evidence of wrongdoing.

o Secure corporate systems from further misuse.

o Identify individuals responsible for engaging in inappropriate acts taken with or without corporate computing systems.

o Protect and secure electronic evidence from intentional or accidental modification or destruction.

Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes provides a set of varied resources for anyone required to look under the hood and behind closed doors of a virtual world to gather evidence and to establish credible audit trails of electronic wrong doing. Knowing how to identify, gather, document, and preserve evidence of electronic tampering and misuse makes reading this book and using the forensic audit procedures it discusses essential to protecting corporate assets."

Title:

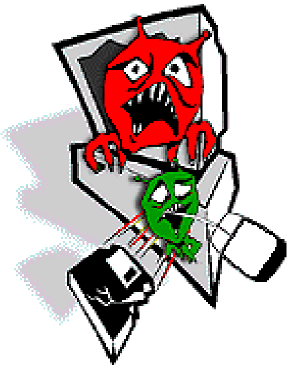
Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes.

Editors:
Albert J. Marcella &
Robert S. Greenfield

Cost:
$54.95

Publisher:
Auerbach Publications

Viruses still on the Rise



According to ICSA Labs, its 7th annual survey of 300 North American organizations identified nearly 1.2 million incidents involving destructive computer code on approximately 666,327 machines during the 20 months from January 2000 through August 2001.

ICSA, a software research firm based in Herndon, VA, indicates that 113 viruses per 1,000 computers, or roughly 13 percent more than reported in their previous annual survey, were reported. Based on previous annual surveys, the data indicates an annual growth rate of approximately 20 virus ncounters per month for every 1,000 PCs.

ICSA was quick to warn that their findings may be dramatically understated, since results were quantified prior to introduction of some of the most dangerous viruses, such as Nimda, which resulted in estimed losses of over $590 million dollars to companies worldwide.

Internet Pirate Pleads Guilty

On February 28, 2002, United States Attorney Paul J. McNulty, Eastern District of Virginia, and Michael Chertoff, Assistant Attorney General for the Criminal Division of the Department of Justice, announced the first guilty plea in the largest international online copyright piracy investigation conducted by federal law enforcement.

John Sankus, Jr., age 28, of Philadelphia, Pennsylvania, co-leader of one of the oldest organized software piracy groups on the Internet, pled guilty to one felony count of conspiracy to commit criminal copyright infringement before U.S. District Court Judge Leonie M. Brinkema this morning. Sankus, who will be sentenced on May 17, 2002, at 9:00 am, could receive a maximum sentence of five years in federal prison and a $250,000 fine.

Sankus was the co-leader of an international Internet software piracy group known as DrinkOrDie. DrinkOrDie engaged in the illegal distribution of copyrighted software, games and movies over the Internet, specializing in being the first to release high-end software applications and utilities. DrinkOrDie is one of many highly structured, security conscious organizations that illegally reproduce and distribute hundreds of thousands of copies of copyrighted works around the world worth billions of dollars in losses each year. Members rarely meet in person and frequently only know each other through their screen nicknames.

"This is a crime against the integrity of our electronic infrastructure," said U.S. Attorney Paul McNulty. "It is imperative that we stop these "techno-gangs" from exploiting new technologies for criminal purposes. This plea is another significant step in our effort to eliminate intellectual property crime on the Internet and to make it safe for individuals and businesses to develop and use new software and technologies."

As part of the plea agreement, the United States and Sankus agreed that the amount of damage attributable to the defendant's actions, during the period charged, exceeds $2.5 million but is less than $5 million.

As co-leader of DrinkOrDie, Sankus was principally responsible for the management and supervision of the day-to-day operations of the criminal enterprise. Sankus supervised approximately 60 individuals who acquired, cracked, and distributed ("released") the pirated software. Company insiders ("suppliers") often provided the group with new software, frequently days or weeks before the software would be released to the general public. Group members known as "crackers" would defeat the software's embedded copyright protections, allowing the software to be illegally reproduced and used by anyone obtaining a copy. The finished product was then quickly distributed to sites located throughout the world for further distribution to an ever-expanding web of sites. Within hours, a new release could be found on hundreds of illegal sites throughout the world.

DrinkorDie concealed these sites and conducted business in closed invite-only Internet relay chat channels. Sankus and other high ranking members of DrinkOrDie used encryption to conceal all e-mails discussing the group's illegal activities. "John Sankus and his group knew what they were doing was illegal and they took every technological step possible to conceal their activity," said McNulty.

DrinkOrDie was the primary group targeted by "Operation Buccaneer," a 15-month undercover investigation by the United States Customs Service with assistance from the Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) and the United States Attorney's Office for the Eastern District of Virginia.

On December 11th, the primary investigative phase of Operation Buccaneer culminated in the simultaneous execution worldwide of over 70 search warrants against targets of the investigation. To date, warrants and/or arrests have been executed in the United States, Australia, Norway, Sweden, the United Kingdom and Finland. Numerous targets of the investigation were arrested and taken into custody in the United Kingdom and investigations are currently ongoing in each of these countries. "Operation Buccaneer brought to light the severity and scope of a multi-billion-dollar software swindle perpetrated over the Internet," said U.S.Customs Commissioner Robert C. Bonner. "This investigation is the first of several cases by the U.S. Customs Service to dismantle the top groups engaged in this illegal activity."

Marty Stansell-Gamm, Chief of CCIPS, said, "The Internet makes it essential for law en-

"This is a crime against the integrity of our electronic infrastructure," said U.S. Attorney Paul McNulty. "It is imperative that we stop these "techno-gangs" from exploiting new technologies for criminal purposes."

Internet Pirate Pleads Guilty

Continued from Page 4

forcement to cooperate across-international borders in order to effectively target all members of these warez groups. Operation Buccaneer is an excellent example of how international cooperation can result in effective criminal enforcement on a global scale. We are committed to protecting the intellectual property rights of this country and will continue to work diligently, both here and abroad, to investigate and prosecute those individuals and groups who traffic in pirated products."

In addition to the plea agreement entered this morning, the United States Attorney expects additional prosecutions in the Eastern District of Virginia as a result of the first phase of Operation Buccaneer.

Former Administrator Charged for 'Time Bomb'

On February 26, 2002, the U.S. Department of Justice announced that a former computer network administrator was sentenced to 41 months in prison for unleashing a $10 million "time bomb" that deleted all the production programs of a New Jersey-based high-tech measurement and control instruments manufacturer, Newark U.S. Attorney Christopher J. Christie announced.

U.S. District Judge William H. Walls ordered Timothy Allen Lloyd, 39, of Wilmington, Del., to surrender on May 1 and begin serving his sentence.

Lloyd was the former chief computer network program designer for Omega Engineering Corp., a Bridgeport, Gloucester County, corporation with offices in Stamford, Conn. On May 9, 2000, a federal jury in Newark convicted Lloyd of one count of fraud and related activity in connection with computers, according to Assistant U.S. Attorney V. Grady O'Malley, who tried the case.

The count on which Lloyd was convicted charged that on July 30, 1996, Lloyd intentionally caused irreparable damage to Omega's financial position by activating a "time bomb" that permanently deleted all of the company's sophisticated manufacturing software programs.

Lloyd had been terminated from Omega on July 10, 1996, after working for the company for approximately 11 years. His Indictment stated that the sabotage resulted in a loss to Omega of at least $10 million in sales and future contracts.

The jury convicted Lloyd after about 12 hours of deliberation over three days. Lloyd was found not guilty of Count Two, transporting approximately $50,000 worth of computer equipment stolen from Omega to his Delaware residence.

At the time of conviction, the case was believed to be one of the most expensive computer sabotage cases in U.S.Secret Service history, according to C. Danny Spriggs, Special Agent in Charge of the U.S. Secret Service's Philadelphia Office.

Lloyd faced a maximum sentence of five years in federal prison on the count of conviction and a $250,000 fine. However, Judge Walls determined the actual sentence based on a formula that took into account the severity and characteristics of the offense as well as other factors. Parole has been abolished in the federal system. Under Sentencing Guidelines, defendants who are given custodial terms must serve nearly all that time.

Christie credited Special Agents of the Secret Service in Philadelphia under the direction of Spriggs, for developing the case against Lloyd.

A publication of the DCIS Northeast Field Office

Defense Criminal Investigative Service
Northeast Field Office
10 Industrial Highway, Bldg. G, Mail Stop 75
Lester, PA 19113

Phone: (610) 595-1900
Fax: (610) 595-1934

Send comments to: Jives@dodig.osd.mil

We're on the Web!
www.dodig.osd.mil/dcis/dcismain.html

The Defense Criminal Investigative Service

"Protecting America's Warfighters"

The Defense Criminal Investigative Service is the investigative arm of the U.S. Department of Defense, Office of the Inspector General. As such, DCIS investigates criminal, civil, and administrative violations impacting the Defense Department. Typically, DCIS investigations focus upon computer crime involving U.S. military and civilian DoD systems, contract procurement fraud, bribery and corruption, health care fraud, anti-trust investigations, significant thefts of government property, export enforcement violations, terrorism related issues impacting DoD, environmental violations, and other issues that impact the integrity and effectiveness of the U.S. Department of Defense.

If you encounter issues that impact the U.S. Department of Defense, please call the DCIS office within your region.

DCIS Northeast Field Office.
10 Industrial Hwy., Bldg. G
Lester, PA 19113
Phone: (610) 595-1900
Fax: (610) 595-1934

DCIS Boston Resident Agency
Rm. 327, 495 Summer Street
Boston, MA 02210
Phone: (617) 753-3044
Fax: (617) 753-4284

DCIS Hartford Resident Agency
525 Brook Street, Suite 205
Rocky Hill, CT 06067
Phone: (860) 721-7751
Fax: (860) 721-6327

DCIS New Jersey Resident Agency
Wick Plaza 1, 100 Dey Pl., Ste. 102
Edison, NJ 08817
Phone: (732) 819-8455
Fax: (732) 819-9430

DCIS New York Resident Agency
One Huntington Quad, Suite 2C01
Melville, NY 11747
Phone: (516) 420-4302
Fax: (516) 420-4316

DCIS Pittsburgh Post of Duty
1000 Liberty Ave., Ste. 1310
Pittsburgh, PA 15222
Phone: (412) 395-6931
Fax: (412) 395-4557

DCIS Syracuse Resident Agency
441 S. Selina St., Ste. 304
Syracuse, NY 13202
Phone: (315) 423-5019
Fax: (315) 423-5099